KPMG

On the 2024 audit committee agenda

KPMG Board Leadership Center

December 7, 2023

The business and risk environment has changed dramatically over the past year, with greater geopolitical instability, surging inflation, high interest rates, and unprecedented levels of disruption.

Audit committees can expect their company's financial reporting, compliance, risk, and internal control environment to be put to the test by an array of challenges—from global economic volatility and the wars in Ukraine and the Middle East to cybersecurity risks and ransomware attacks and preparations for US and global climate and sustainability reporting requirements, which will require developing related internal controls and disclosure controls and procedures.

Drawing on insights from our interactions with audit committees and business leaders, we highlight eight issues to keep in mind as audit committees consider and carry out their 2024 agendas:

- **Stay focused on financial reporting and related internal control risks—job number one.**
- **Clarify the roles of management's disclosure committee and ESG teams and committees in preparations for new US, state, and global climate and other sustainability disclosures—and oversee the quality and reliability of the underlying data.**
- **Monitor management's preparations for and compliance with the SEC's cybersecurity rules.**
- **Define the audit committee's oversight responsibilities for generative artificial intelligence (AI).**
- **Focus on leadership and talent in the finance organization.**
- **Reinforce audit quality and stay abreast of proposed changes to PCAOB auditing standards, including its proposal relating to noncompliance with laws and regulations.**
- **Make sure internal audit is focused on the company's key risks—beyond financial reporting and compliance—and is a valued resource to the audit committee.**
- **Help sharpen the company's focus on ethics, compliance, and culture.**

Stay focused on financial reporting and related internal control risks—job number one.

Focusing on the financial reporting, accounting, and disclosure obligations posed by the current geopolitical, macroeconomic, and risk landscape will be a top priority and major undertaking for audit committees in 2024. Key areas of focus for companies' 2023 10-K and 2024 filings should include:

Forecasting and disclosures. Among the matters requiring the audit committee's attention are disclosures regarding the impact of the wars in Ukraine and the Middle East, government sanctions, supply chain disruptions, heightened cybersecurity risk, inflation, interest rates, market volatility, and the risk of a global recession; preparation of forward-looking cash-flow estimates; impairment of nonfinancial assets, including goodwill and other intangible assets; impact of events and trends on liquidity; accounting for financial assets (fair value); going concern; and use of non-GAAP metrics. With companies making more tough calls in the current environment, regulators are emphasizing the importance of well-reasoned judgments and transparency, including contemporaneous documentation to demonstrate that the company applied a rigorous process. Given the fluid nature of the long-term environment, disclosure of changes in judgments, estimates, and controls may be required more frequently.

In reviewing management's disclosures regarding these matters, consider the questions posed by the staff of the SEC's Division of Corporation Finance in its May 2022 sample letter pertaining to the Russia-Ukraine war and its July 2023 sample letter regarding China-specific disclosures. The sample comment letters may be instructive in considering the company's disclosure obligations posed by the wars in Ukraine, the Middle East (and the risk of a regional war), and the broader geopolitical, macroeconomic, and risk environment.

Internal control over financial reporting (ICOFR) and probing control deficiencies. Given the current risk environment, as well as changes in the business, such as acquisitions, new lines of business, digital transformations, etc., internal controls will continue to be put to the test. Discuss with management how the current environment and regulatory mandates—including new climate and cybersecurity rules—affect management's disclosure controls and procedures and ICOFR, as well as management's assessment of the effectiveness of ICOFR. When control deficiencies are identified, probe beyond management's explanation for "why it's only a control deficiency" or "why it's not a material weakness" and help provide a balanced evaluation of the deficiency's severity and cause. Is the audit committee—with management—regularly taking a fresh look at the company's control environment? Have controls kept pace with the company's operations, business model, and changing risk profile, including cybersecurity risks?

Importance of a comprehensive risk assessment. SEC Chief Accountant Paul Munter released a statement highlighting the importance of a comprehensive risk assessment by management and auditors—particularly, the SEC's concerns about auditors and management appearing to be too narrowly focused on information and risks that directly impact financial reporting while disregarding broader, entity-level issues that may also impact financial reporting and internal controls. Munter's statement discussed management's obligations with respect to ongoing risk assessments and addressed auditors' responsibility as gatekeepers to hold management accountable in the public interest.

Committee bandwidth and skill sets. The audit committee's role in overseeing management's preparations for new US, state, and global climate and other sustainability reporting requirements, coupled with its role in overseeing new SEC cybersecurity disclosures, further expands the committee's oversight responsibilities beyond its core oversight responsibilities (financial reporting and related internal controls, and internal and external auditors). This expansion should heighten concerns about audit committee bandwidth and "agenda overload." Reassess whether the committee has the time and expertise to oversee the major risks on its plate today. Such a reassessment is sometimes done in connection with an overall reassessment of issues assigned to each board standing committee. For example, do cybersecurity, climate, sustainability, or "mission-critical" risks such as safety, as well as AI, including generative AI, require more attention at the full board level—or perhaps the focus of a separate board committee? The pros and cons of creating an additional committee should be weighed carefully, but considering whether a finance, technology, risk, climate and sustainability, or other committee—and perhaps the need for directors with new skill sets—would improve the board's effectiveness can be a healthy part of the risk oversight discussion.

Reassess whether the audit committee has the time and expertise to oversee the major risks on its plate today.

Clarify the roles of management's disclosure committee and ESG teams and committees in preparations for new US, state, and global climate and other sustainability disclosures—and oversee the quality and reliability of the underlying data.

As discussed in On the 2024 board agenda, an important area of board focus and oversight will be management's efforts to prepare for US, state, and global regulatory mandates that will dramatically increase climate and other sustainability disclosure requirements for US companies.

While US companies await final SEC climate rules, they are preparing to comply with California climate legislation signed into law in October 2023, and US companies with international operations are also assessing the potential impacts of, and preparing for compliance with, European Sustainability Reporting Standards (ESRSs) issued under the EU's Corporate Sustainability Reporting Directive (CSRD)—which covers a broad range of sustainability issues beyond climate—and IFRS® Sustainability Disclosure Standards issued by the International Sustainability Standards Board (ISSB), as well as other foreign disclosure regimes. Countries are already announcing adoption of, or commitments to consider adopting, the final ISSB standards, including Australia (climate only), Brazil, Japan, and the UK.

The California laws and international climate standards, as well as the anticipated SEC climate rules—which will likely vary in important respects and have different effective dates—are based in part on the standards and frameworks of the Task Force on Climate-related Financial Disclosures (the TCFD) and the Greenhouse Gas (GHG) Protocol and are highly prescriptive and expansive. Detailed disclosures in a number of areas would be required, including GHG emissions data (Scopes 1 and 2, and in many cases, Scope 3), with third-party assurance, as well as detailed disclosures about the impacts of climate-related risks and transition risks on the business, financials, strategy, and business model.

In the near term, US companies must determine which standards apply, effective dates, and the level of interoperability of the applicable standards. Monitoring SEC, state, and international developments will be critical. A key area of board and audit committee focus will be the state of the company's preparedness—requiring periodic updates on management's preparations, including gap analyses, resources, and skills/talent requirements to meet regulatory deadlines. In addition to the compliance challenge, companies must consider whether disclosures are consistent, and the potential for liability posed by detailed disclosures—as well as the US implications of a company making more detailed disclosures in another jurisdiction (such as the EU or under state laws).

This will be a major undertaking, with cross-functional management teams involved, including management's disclosure committee and management's ESG team/committee—often led by an ESG controller at larger companies—with multiple board committees overseeing

different aspects of these efforts. Given the scope of the effort, audit committees should encourage management's disclosure committee and management's ESG team/committee to prepare now by developing management's path to compliance with applicable reporting standards and requirements—including management's plan to develop high-quality, reliable climate and sustainability data. Key areas of audit committee focus should include:

- Clarifying the disclosure committee's role and responsibilities in connection with disclosures contained in SEC and other regulatory filings and those made voluntarily in sustainability reports, websites, etc., including coordination with cross-functional management ESG team(s) or committee(s). Since disclosures that are not filed still carry potential liability, management should have processes in place to review these disclosures, including for consistency with filed disclosures.
- Reassessing the composition of the disclosure committee. Given the US, state, and global climate and other sustainability reporting requirements and the intense focus on these disclosures generally, companies should consider expanding management's disclosure committee or creating a subcommittee to include appropriate climate and other sustainability functional leaders, such as the ESG controller (if any), chief sustainability officer, chief human resources officer, chief diversity officer, chief supply chain officer, and chief information security officer.
- Encouraging management's disclosure committee to work with management's ESG team/committee to identify gaps, consider how to gather and maintain quality information, and closely monitor US, state, and global rulemaking activities.
- Expanding management's subcertification process to support CEO and CFO quarterly 302 certifications regarding design and operational effectiveness of disclosure controls and procedures.
- Understanding whether appropriate systems are in place or are being developed to ensure the quality of data that must be assured by third parties.

Monitor management's preparations for and compliance with the SEC's cybersecurity rules.

The SEC's rules require several new and enhanced disclosures on cybersecurity risk management, strategy, governance, and incident reporting. Companies must disclose new information in two broad categories.

Companies are required to **disclose material "cybersecurity incidents" on Form 8-K,** within four business days after the company determines that the incident was material—not from the time of discovery of the incident. Companies must make materiality determinations "without unreasonable delay" after discovery of the incident.

Companies are required to **disclose material information regarding their cybersecurity risk management, strategy, and governance in their annual reports on Form 10-K.** While companies will not be required to disclose board-level cybersecurity expertise, they will be required to describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats.

Companies—other than smaller reporting companies—must begin complying with the incident disclosure requirements on December 18, 2023. Smaller reporting companies must begin complying on June 15, 2024. All public companies will be required to make Form 10-K annual disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023.

As companies finalize their preparations for these disclosures, we highlight the following areas for the audit committee's attention:

Cybersecurity risk management, strategy, and governance disclosures on Form 10-K. The preparation of these disclosures will take time and care, as the disclosures are detailed and extensive and will likely require a reassessment, and perhaps modification, of the company's existing risk management and governance processes, including board oversight processes. Boards

should be working with management now as management prepares for the upcoming Form 10-K disclosures.

Management's cyber incident response plan. Management's cyber incident response policies and procedures, including disclosure controls and procedures and internal controls, must be reviewed and updated to provide for the timely consideration of materiality—at the same time that management may be engaged in remediation and investigation efforts. This would include a clear delineation of the responsibilities of management's cybersecurity and risk management teams, management's disclosure committee, and the legal department, as well as escalation procedures for determining materiality and the preparation and

review of disclosures. Escalation protocols should provide for information from the technology team to be promptly provided to the cross-functional team making materiality determinations, and also address when the board is notified and how internal and external communications are handled. Management and the board should conduct periodic tabletop exercises to test management's response plans and procedures, including protocols for documenting incidents, evaluating for materiality, and drafting Form 8-K disclosures—and refine response plans and procedures to reflect what is learned from those exercises. Incident response plans should also be updated to take into account the changing cyber risk landscape.

Consideration of "materiality." While the definition of materiality has not changed, applying that standard in the context of a cybersecurity incident is not straightforward. In its final release, the SEC said that companies should consider qualitative factors in assessing the material impact of an incident, and indicated that harm to a company's reputation, customer or vendor relationships, or competitiveness, and the possibility of litigation or regulatory investigations or actions, may be examples of material impacts. Audit committees should confirm that management has in place policies and procedures for the cross functional team making materiality determinations, including procedures for the identification of significant cyber incidents that should be escalated and discussed with management's disclosure committee and legal team for final materiality determination, and documenting its materiality determinations. Companies may want to consider, in advance, what might constitute a material incident.

The role of management's disclosure committee. Consider the role and responsibilities of management's disclosure committee in developing and maintaining cybersecurity-related disclosure controls and internal controls and procedures. What resources and processes does the committee require to make a timely determination of materiality in the event of a cyber incident?

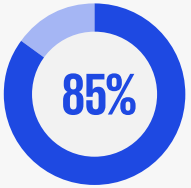
Define the audit committee's oversight responsibilities for generative AI.

As discussed in On the 2024 board agenda, oversight of generative AI will be an oversight priority for almost every board in 2024. Many boards are considering how to oversee generative AI at the full-board and committee levels.

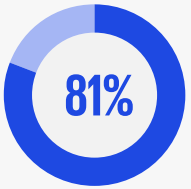
The audit committee may end up overseeing compliance with the patchwork of differing laws and regulations governing generative AI, as well as the development and maintenance of related internal controls and disclosure controls and procedures. Some audit committees may have broader oversight responsibilities for generative AI, including oversight of various aspects of the company's governance structure for the development and use of the technology. How and when is a generative AI system or model—including a third-party model—developed and deployed, and who makes that decision? What generative AI risk management framework is used? Does the organization have the necessary generative AI–related talent and resources?

Given how fluid the situation is—with generative AI gaining rapid momentum—the allocation of oversight responsibilities to the audit committee may need to be revisited.

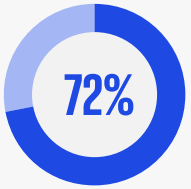
KPMG 2023 US CEO Outlook findings



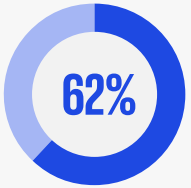
say AI can help detect cyberattacks while providing new attack strategies for adversaries.



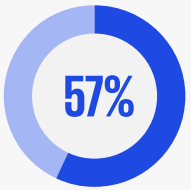
express concern that the lack of regulation for generative AI within their industry will hinder their organization's success.



say generative AI is a top investment priority despite uncertain economic conditions.



expect to see returns from their investments in 3 to 5 years.



are placing capital investment in buying new technology.

Source: KPMG LLP, KPMG 2023 US CEO Outlook, October 2023, p. 6.

Focus on leadership and talent in the finance organization.

Finance organizations face a challenging environment—addressing talent shortages, while at the same time managing digital strategies and transformations and developing robust systems and procedures to collect and maintain high-quality climate and sustainability data both to meet investor and other stakeholder demands and in preparation for US, state, and global disclosure requirements. At the same time many are contending with difficulties in forecasting and planning for an uncertain environment.

As audit committees monitor and help guide finance's progress in these areas, we suggest two areas of focus:

- Many finance organizations have been assembling or expanding management teams or committees charged with managing a range of climate and other sustainability activities, and preparing for related US, state, and global disclosure rules—e.g., identifying and recruiting climate and sustainability talent and expertise, developing internal controls and disclosure controls and procedures, and putting in place technology, processes, and systems.
- At the same time, the acceleration of digital strategies and transformations presents important opportunities for finance to add greater value to the business. The finance function is combining strong analytics and strategic capabilities with traditional financial reporting, accounting, and auditing skills.

It is essential that the audit committee devote adequate time to understanding finance's climate/sustainability strategy and digital transformation strategy and help ensure that finance is attracting, developing, and retaining the leadership, talent, skill sets, and bench strength to execute those strategies, as well as its existing responsibilities. Staffing deficiencies in the finance department may pose the risk of an internal control deficiency, including a material weakness.

Reinforce audit quality and stay abreast of proposed changes to PCAOB auditing standards, including its proposal relating to noncompliance with laws and regulations.

Audit quality is enhanced by a fully engaged audit committee that sets the tone and clear expectations for the external auditor and monitors auditor performance rigorously through frequent, quality communications and a robust performance assessment.

In setting expectations for 2024, audit committees should discuss with the auditor how the company's financial reporting and related internal control risks have changed in light of the geopolitical, macroeconomic, regulatory and risk landscape, as well as changes in the business.

Set clear expectations for frequent, open, candid communications between the auditor and the audit committee, beyond what's required. The list of required communications is extensive and includes matters about the auditor's independence as well as matters related to the planning and results of the audit. Taking the conversation beyond what's required can enhance the audit committee's oversight, particularly regarding the company's culture, tone at the top, and the quality of talent in the finance organization.

Audit committees should also probe the audit firm on its quality control systems that are intended to drive sustainable, improved audit quality—including the firm's implementation and use of new technologies such as AI to drive audit quality. In discussions with the external auditor regarding the firm's internal quality control system, consider the results of PCAOB inspections, Part I and Part II, and internal inspections and efforts to address deficiencies. Remember that audit quality is a team effort requiring the commitment and engagement of everyone involved in the process—the auditor, audit committee, internal audit, and management.

In June, the PCAOB proposed sweeping changes to auditing standards that would heighten the auditor's responsibilities for detecting legal and regulatory noncompliance and alerting appropriate members of management and the audit committee when instances of noncompliance with laws and regulations (NOCLAR) are identified. The public comment deadline ended August 7.

Audit committees need to understand the practical implications of the PCAOB's proposed amendments. The proposal would materially increase the work of the auditor—going beyond the auditor's traditional areas of expertise—and impact the company's existing internal processes for monitoring legal and regulatory compliance that might not be material or affect the financial statements. According to the Center for Audit Quality (CAQ), "this is the most significant PCAOB proposal since their 2011 Concept Release on mandatory firm rotations." The CAQ is encouraging the PCAOB to further engage with all stakeholders—auditors, management, audit committees—to better understand the implications of the proposal and whether it will meet the PCAOB's objectives.

Make sure internal audit is focused on the company's key risks—beyond financial reporting and compliance—and is a valued resource to the audit committee.

As audit committees wrestle with heavy agendas—and risk management is put to the test—internal audit should be a valuable resource for the audit committee and a crucial voice on risk and control matters. This means not just focusing on financial reporting and compliance risks, but also critical operational and technology risks and related controls, as well as ESG risks.

ESG-related risks are rapidly evolving and include human capital management—from diversity, equity, and inclusion (DEI) to talent, leadership, and corporate culture—as well as climate, cybersecurity, data governance and data privacy, and risks associated with ESG disclosures. Disclosure controls and procedures and internal controls should be a key area of internal audit focus. Clarify internal audit's role in connection with ESG risks and enterprise risk management more generally—which is not to manage risk, but to provide added assurance regarding the adequacy of risk management processes. Do management teams have the necessary resources and skill sets to execute new climate and ESG initiatives?

Reassess whether the internal audit plan is risk based and flexible enough to adjust to changing business and risk conditions. The audit committee should work with the chief audit executive and chief risk officer to help identify the risks that pose the greatest threat to the company's reputation, strategy, and operations, and to help ensure that internal audit is focused on these key risks and related controls. These may include industry-specific, mission-critical, and regulatory risks, economic and geopolitical risks, the impact of climate change on the business, cybersecurity and data privacy, risks posed by generative AI and digital technologies, talent management and retention, hybrid work and organizational culture, supply chain and third-party risks, and the adequacy of business continuity and crisis management plans.

Given internal audit's broadening mandate, it will likely require upskilling. Set clear expectations and help ensure that internal audit has the talent, resources, skills, and expertise to succeed—and help the chief audit executive think through the impact of digital technologies on internal audit.

Work with the chief audit executive and chief risk officer to help identify the risks that pose the greatest threat to the company's reputation, strategy, and operations, and to help ensure that internal audit is focused on these key risks and related controls.

Help sharpen the company's focus on ethics, compliance, and culture.

The reputational costs of an ethics or compliance failure are higher than ever, particularly given increased fraud risk, pressures on management to meet financial targets, and increased vulnerability to cyberattacks. Fundamental to an effective compliance program is the right tone at the top and culture throughout the organization, including commitment to its stated values, ethics, and legal and regulatory compliance. This is particularly true in a complex business environment as companies move quickly to innovate and capitalize on opportunities in new markets, leverage new technologies and data, and engage with more vendors and third parties across complex supply chains.

Closely monitor the tone at the top and culture throughout the organization with a sharp focus on behaviors (not just results) and yellow flags. Is senior management sensitive to ongoing pressures on employees (both in the office and at home), employee health and safety, productivity, and employee engagement and morale? Leadership, communication, understanding, and compassion are essential. Does the company's culture make it safe for people to do the right thing? It is helpful for directors to spend time in the field meeting employees to get a better feel for the culture. Help ensure that the company's regulatory compliance and monitoring programs are up to date and take into account the updated US sentencing guidelines, cover all vendors in the global supply chain, and communicate the company's expectations for high ethical standards.

Focus on the effectiveness of the company's whistleblower reporting channels (including whether complaints are being submitted) and investigation processes. Does the audit committee see all whistleblower complaints? If not, what is the process to filter complaints that are ultimately reported to the audit committee? With the radical transparency enabled by social media, the company's culture and values, commitment to integrity and legal compliance, and its brand reputation are on full display.

Leadership, communication, understanding, and compassion are essential.

Contact us

John H. Rodi
Leader, KPMG Board Leadership Center

Stephen Dabney
Leader, KPMG Audit Committee Institute

KPMG Board Leadership Center Senior Advisors

Claudia Allen

Susan Angele

Annalisa Barrett

Stephen Brown

Patrick Lee

About the KPMG Board Leadership Center

The KPMG Board Leadership Center (BLC) champions outstanding corporate governance to drive long-term value and enhance stakeholder confidence. Through an array of insights, perspectives, and programs, the BLC—which includes the KPMG Audit Committee Institute and close collaboration with other leading director organizations—promotes continuous education and improvement of public and private company governance. BLC engages with directors and business leaders on the critical issues driving board agendas—from strategy, risk, talent, and ESG to data governance, audit quality, proxy trends, and more. Learn more at kpmg.com/us/blc.

About the KPMG Audit Committee Institute

As part of the KPMG Board Leadership Center, the ACI provides audit committee and board members with practical insights, resources, and peer-exchange opportunities focused on strengthening oversight of financial reporting and audit quality, and the array of challenges facing boards and businesses today—from risk management and emerging technologies to strategy, talent, and global compliance. Learn more about ACI at kpmg.com/us/aci.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia